WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
GREGORY M. NESPOLE (*pro hac vice application forthcoming*)
MICHAEL LISKOW (*pro hac vice application forthcoming*)
270 Madison Avenue
New York, New York 10016
Tel. (212) 545-4600
Facsimile : (212) 545-4653
Email : nespole@whafh.com
liskow@whafh.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
CARL MALMSTROM (*pro hac vice application forthcoming*)
70 W. Madison St., Suite 1400
Chicago, IL 60603
Tel. (312) 984-0000
Facsimile: (312) 214-3110
Email: malmstrom@whafh.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
RACHELE R. RICKERT (*pro hac vice application forthcoming*)
750 B Street, Suite 2770
San Diego, CA 92101
Tel. (619) 239-4599
Email: rickert@whafh.com

BICKERTON DANG, LLLP
JAMES J. BICKERTON 3085
BRIDGET G. MORGAN 8705
745 Fort Street, Suite 801
Honolulu, Hawaii 96813
Tel. (808) 599-3811
Email : bickerton@bsds.com
morgan@bsds.com

Attorneys for Plaintiffs
JOSHUA BOKELMAN and SUCHANDRA THAPA,
Individually and on behalf of all others similarly situated

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAI'I

JOSHUA BOKELMAN and SUCHANDRA THAPA, individually and on behalf of all others similarly situated, Plaintiffs, vs. FCH ENTERPRISES, INC. Defendant.	Civil No. _____ (Class Action) **COMPLAINT; DEMAND FOR JURY TRIAL; SUMMONS**

COMPLAINT

Plaintiffs Joshua Bokelman and Suchandra Thapa ("Plaintiffs"), individually and on behalf of similarly situated individuals (the "Class" defined below), allege upon personal knowledge as to themselves and their own actions, and upon information and belief as to the Class, including the investigation of counsel, as follows:

NATURE OF ACTION

1. Defendant FCH Enterprises, Inc. ("Defendant") is the owner of Zippy's Restaurants, one of the largest local restaurant chains in Hawai'i. There are 24 Zippy's restaurants in the Hawaiian Islands, most of which include a bakery counter – called Napoleon's Bakery – and two of which include a sushi bar

(Kahala Sushi and Pearl City Sushi). Defendant also owns a banquet hall called Pōmaika'i Ballrooms. At least tens of thousands of people patronize Defendant's locations throughout the Hawaiian Islands every year.

2. On April 27, 2018, Defendant announced a data breach affecting customers who used a credit or debit card at all of its Zippy's locations (including Napoleon's Bakery, Kahala Sushi, Pearl City Sushi) and "a small number of credit and debit cards used to purchase drinks at events held at the Pomaika'i Ballrooms" from November 23, 2017 to March 29, 2018 (the "Class Period").

3. The data breach included cardholders' names, card numbers, expiration dates, and security codes – everything needed by a thief to use those credit and debit cards fraudulently. This sensitive personal information ("SPI") of Plaintiffs and the Class can be used to make fraudulent charges or even open unauthorized new accounts. Along with actual financial loss, such charges and unauthorized activity can also lead to a lowering of one's credit score.

4. Indeed, several people who have posted on websites such as Reddit.com and who have responded to news articles from local media sources have publicly stated that they suspect recent fraudulent charges come from using their payment cards at Defendant's restaurants during the Class Period.

5. Defendant admits that it was first alerted to this data breach on March 9, 2018, though it inexplicably delayed informing its customers of the breach for

nearly 50 days – until April 27, 2018. Moreover, despite Defendant learning about the breach on March 9, 2018, credit cards used for purchases up to 20 days later, March 29, 2018, continued to be affected by the breach.

6. Defendant has made public statements apologizing for the breach and encouraging customers to monitor their account activity, but to date has not made any effort to assist or recompense affected customers.

7. Defendant failed to follow industry best practices for the protection of point-of-sale ("POS") customer data. As a result, Defendant inadequately protected the SPI of its customers and allowed it to be stolen by hackers.

8. Plaintiffs and the Class they seek to represent seek damages and restitution for the loss suffered due to Defendant's actions, injunctive relief ordering Defendant to secure the SPI it collects in an appropriate and sufficient manner, as well as actual damages and attorneys' fees for violations of Haw. Rev. Stat. § 487N, *et seq.*, the Hawaii Data Breach Notification Act, and Haw. Rev. Stat. § 481A-1, *et seq.*, the Hawaii Uniform Deceptive Trade Practice Act.

PARTIES

9. Plaintiff Joshua Bokelman is a citizen of Hawaii, domiciled in Honolulu County. Plaintiff Bokelman made numerous purchases at the Zippy's at 98-048 Kamehameha Highway in Aiea during the period Class Period using his debit card, a location Defendant has confirmed was affected by the data breach,

including on March 20, 2018. Plaintiff Bokelman has since incurred more than $300 in fraudulent debit card charges to his account. Plaintiff Bokelman's only debit purchases using his debit card were made at Zippy's during the Class Period as all other transactions made by Plaintiff connected to his debit card were made using Apple Pay. Upon information and belief, Zippy's does not accept Apple Pay as a manner of payment at its stores. In addition, Apple Pay utilizes a one-time encrypted authorization code generated for each transaction rather than transmitting the debit or credit card number (and attendant expiration date and security code) between the customer and the vendor. Plaintiff Bokelman's SPI was accessed as a result of Defendant's data breach, and Plaintiff Bokelman has both suffered damage as a result of the breach and stands at imminent risk of further fraud or identity theft.

10. Plaintiff Suchandra Thapa is a citizen of Illinois, domiciled in Cook County. On February 4, 2018, Plaintiff Thapa used his credit card at the Zippy's at 1725 S. King St. in Honolulu, a location Defendant has confirmed was affected by the data breach. On February 21, 2018, Plaintiff Thapa incurred fraudulent charges on the account for the Chase credit card that he used at Zippy's. Plaintiff Thapa's fraudulent charges were later removed by Chase and he waited a few days to receive a new credit card. Plaintiff Thapa's SPI was accessed as a result of

Defendant's data breach, and Plaintiff Thapa stands at imminent risk of fraud or identity theft through the use of his SPI by hackers.

11. Defendant FCH Enterprises, Inc. is a privately-held for-profit corporation established in 1966 which is headquartered at and has its registered agent located at 1765 S. King St., Honolulu, Hawai'i, 96826. Defendant is a Hawai'i corporation and does business throughout the State of Hawai'i as "Zippy's Restaurants," "Napoleon's Bakery" as well as "Kahala Sushi," "Pearl City Sushi," and "Pomaika'i Ballrooms."

JURISDICTION AND VENUE

12. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) ("The Class Action Fairness Act") because sufficient diversity of citizenship exists between parties in this action, the aggregate amount in controversy exceeds $5,000,000, and there are 100 or more members of the Class.

13. This Court has personal jurisdiction over Defendant because it is incorporated in Hawai'i, has its principal office in Hawai'i, and regularly conducts business in Hawai'i.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant is incorporated in this District, has its principal office in this District, and regularly conducts business in this District.

FACTUAL ALLEGATIONS

Defendant's Restaurants and Its Data Collection Practices

15. Defendant's restaurants have operated in Hawaii since 1966[1], and, on information and belief, serve at least tens of thousands of customers per year. Defendant's brands include Zippy's Restaurants, a fast food and fast-casual chain of restaurants specializing in chili and local Hawaiian dishes; Napoleon's Bakery, a pastry counter that operates within Zippy's restaurants; Kahala Sushi and Pearl City Sushi, sushi counters that operate within two Zippy's restaurants; Pomaika'i Ballrooms, a banquet hall as well as a separate catering and food-preparation businesses.

16. Defendant, like most commercial merchants, uses a point-of-sale ("POS") system for customer purchases, which includes cash registers, payment-card readers, POS software and computer infrastructure for conducting payment card transactions.

17. The National Restaurant Association, the primary industry trade group for restaurant chains, subscribes to the best practices published by the PCI Security Standards Council.[2] These standards include encrypting transmissions of

---

[1] *See* http://www.fchenterprises.com/ (last viewed June 1, 2018).

[2] *See* https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security (last viewed June 1, 2018).

cardholder data, maintaining firewalls, **not** storing cardholder data in computers, and using and regularly changing strong passwords on hardware and software. When properly followed, it is virtually impossible for a restaurant to suffer a POS data breach of the nature that Defendant suffered.

The Data Breach

18. Defendant announced that it first learned of the data breach on March 9, 2018.[3] Defendant's announcement included the fact that its independently-contracted forensic expert notified it on April 4, 2018 that all its Zippy's and Napoleon's locations, along with its Pearl City Sushi, Kahala Sushi, and some drink purchases at Pomaika'i Ballrooms, were affected from November 23, 2017 to March 29, 2018. *Id.*[4]

19. Defendant announced that the information involved in the breach included cardholder names, card numbers, expiration dates, and security codes. *Id.* In short, the accessed SPI included everything needed by a hacker to make fraudulent payment card purchases.

---

[3] *See* http://zippys.com/security/ (last viewed June 1, 2018).

[4] Defendant claimed that credit and debit cards used at their companies "A Catered Experience" and "Food Solutions International" were not impacted, and also stated that "[o]rders placed on Zippys' website, payments for senior cards submitted to Zippy's corporate office, fundraisers, and catering orders were also not impacted by this event." *Id.*

20. Defendant has offered no further details about the nature of the breach. Defendant has not informed its customers of the reason it waited until April 27, 2018 to announce the breach publicly, even though it knew about the breach as of March 9, 2018 and had the results of its forensic audit in hand by April 4, 2018. Nor has Defendant explained how, despite Defendant learning about the breach on March 9, 2018, credit cards used for purchases up to 20 days later, March 29, 2018, continued to be captured by the breach.

21. The Hawai'i Office of Consumer Protection (the "OCP") has announced an investigation into the circumstances of the breach.[5] Furthermore, local security experts have noted that Defendant's "process might have been slower than usual," noting that "you want to let your customers know as quickly as possible."[6]

22. Since the breach, Defendant's customers have also complained publicly of fraudulent charges, which they believe are attributable to the breach itself. Some of these fraudulent charges occurred during the window between when Defendant received the results of its audit and when it announced to the public that a data breach had occurred.

---

[5] *See* https://www.bizjournals.com/pacific/news/2018/04/30/hawaii-office-of-consumer-protection-investigates.html (last viewed June 1, 2018).

[6] *See* https://www.bizjournals.com/pacific/news/2018/05/03/what-businesses-can-learn-from-the-zippy-s-data.html (last viewed June 1, 2018).

The Effect of the Data Breach on Plaintiffs and the Class

23. Plaintiffs and the Class now face a real and immediate risk of identity theft and fraudulent payment card charges resulting from Defendant's actions, including its decision to delay public notification of the breach.

24. The processes of discovering and dealing with the repercussions of identity theft and fraudulent payments are time consuming and difficult. The Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[7]

25. The victims here, Plaintiffs and the Class, are no different, as they are faced with an arduous path to secure their SPI in response to Defendant's negligence. As urged by the OCP following Defendant's announcement of the breach, Plaintiffs and the Class must take the following steps to attempt to prevent further misuse of their SPI:

- Review and monitor credit card statements for any unusual or unknown charges.
- Contact their financial institution to determine if there is any suspicious activity on their accounts.
- Change their account information.

[7] Erika Harrell and Lynn Langton, *Victims of Identity Theft, 2012*, (Bureau of Justice Statistics Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf (last viewed June1, 2018).

- Place a fraud alert on their credit bureau reports.
- Place a security freeze on their credit bureau reports.
- Periodically monitor their credit bureau reports for any unusual activity and check for accuracy.[8]

26. Additionally, there is commonly lag time between when harm occurs and when it is discovered and also between when SPI is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[9]

27. There is a very strong probability that those impacted by Defendant's failure to secure the SPI could be at risk of fraud and identity theft for extended periods of time.

28. As a result of Defendant's negligent security practices, Plaintiffs and the Class have been exposed to fraud and have both directly incurred damages and

---

[8] *See* http://cca.hawaii.gov/blog/release-state-office-of-consumer-protection-investigating-security-breach-at-zippys/ (last viewed June 1, 2018).

[9] U.S. Government Accountability Office, GAO Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last viewed June 1, 2018).

face a heightened and imminent risk of fraud and identity theft. Plaintiffs and the Class must now and in the future closely monitor their financial accounts to guard against identity theft and fraudulent charges. Plaintiffs and the Class may be faced with fraudulent debt or incur costs for, among other things, paying monthly or annual fees for identity theft and credit monitoring services and obtaining credit reports, credit freezes, and other protective measures to deter, detect, and mitigate the risk of identity theft and fraud. Some have already incurred costs in doing so.

CLASS ACTION ALLEGATIONS

29. Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), seeking damages and equitable relief on behalf of the following Class:

> All persons whose SPI was accessed and/or compromised by unauthorized individuals as part of the data breach at issue in this litigation.

30. Excluded from the Class are: Defendant, any parent, affiliate, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any of Defendant's officers or directors; any successor or assignee of Defendant; and any entity with whom Defendant contracts for POS services. Also excluded is any Judge assigned to this case.

31. The Class is so numerous that joinder of all members is impracticable. While Plaintiffs do not know the exact number of the members of the Class, Plaintiffs believe it contains hundreds of thousands of members.

32. Common questions of law and fact exist as to all members of the Class. Such questions of law and fact common to the Class include, but are not limited to:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant owed a duty to Plaintiffs and members of the Class to adequately protect their SPI;

c. Whether Defendant breached its duty to adequately protect the SPI of Plaintiffs and members of the Class;

d. Whether Defendant should have known that its data systems and processes were vulnerable to attack and taken sufficient steps to prevent such attack;

e. Whether Defendant's conduct, including its failure to act, was the proximate cause of, or resulted in, the breach of its database containing SPI;

f. Whether Defendant unreasonably delayed notification of the breach at issue in this litigation;

g. Whether Defendant's conduct constituted a violation of Haw. Rev. Stat. § 487N, *et seq.*, the Hawaii Data Breach Notification Act;

h. Whether Defendant's conduct constituted a violation of Haw. Rev. Stat. § 481A-1, *et seq.*, the Hawaii Uniform Deceptive Trade Practice Act;

i. Whether Plaintiffs and members of the Class suffered legally cognizable damages as a result of Defendant's conduct and are entitled to recover damages; and

j. Whether Plaintiffs and members of the Class are entitled to equitable relief.

33. Plaintiffs' claims are typical of the claims of the members of the Class, and Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs and all members of the Class are similarly affected by Defendant's wrongful conduct in that their information was exposed to unauthorized users in violation of federal, state and common law.

34. Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other members of the Class. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other members of the Class. Plaintiffs are represented by counsel who are competent and experienced in the prosecution of security breach and class action litigation.

35. The questions of law and fact common to the members of the Class predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

36. Class action treatment is a superior method for the fair and efficient adjudication of the controversy, in that, among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in management of this class action.

37. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications, establishing incompatible standards of conduct for Defendant.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of Plaintiffs and the Class)

38. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

39. Defendant solicited and took possession of the SPI of Plaintiffs and the Class and had a duty to exercise reasonable care in safeguarding and protecting that information from unauthorized access or disclosure. The duty included maintaining and testing Defendant's security systems and taking other reasonable security measures to protect and adequately secure the SPI from unauthorized access and use. Defendant also had a duty to timely notify Plaintiffs and the Class that their SPI had been or may have been stolen. Defendant further had a duty to destroy the SPI of Plaintiffs and the Class within an appropriate amount of time after it was no longer required in order to mitigate the risk of such non-essential SPI being compromised in a data breach. Defendant finally had a duty to take necessary steps to promptly stop any further breach of customer data once Defendant was made aware of the breach.

40. Defendant's duties arose from its relationship to Plaintiffs and the Class and from industry custom.

41. Defendant, through its actions and/or failures to act, unlawfully breached duties to Plaintiffs and the Class by failing to implement standard industry protocols, to exercise reasonable care to secure and keep private the SPI entrusted to it, to notify Plaintiffs and the Class of the breach as soon as Defendant was made aware of it, and to take any necessary steps to immediately end the ongoing breach once Defendant became aware of it.

42. Defendant's failure to exercise reasonable care in safeguarding the SPI of Plaintiffs and the Class by adopting appropriate security measures, including encryption, was the direct and proximate cause of the SPI of Plaintiffs and the Class being accessed and stolen through the data breach.

43. It was foreseeable that if Defendant or its agents did not take reasonable security measures, the SPI of Plaintiffs and the Class would be stolen. Companies like Defendant face a high threat of data breaches due in part to the large amounts and type of information they store and the value of such information on the black market. Defendant should have known to take all reasonable precautions to secure customers' SPI, especially in light of recent data breaches and publicity regarding such breaches.

44. As a result of Defendant's breach of duties, Plaintiffs and the Class have been injured and have suffered damages, including but not limited to having credit card accounts fraudulently applied for in their names, lowered credit scores, and being required to expend time and money to prospectively and/or remedially address the harm created by the data breach.

45. Defendant's negligence was a substantial factor in causing harm to Plaintiffs and the Class.

46. Plaintiffs and the Class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and any other relief as the Court deems just and proper.

SECOND CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of Plaintiffs and the Class)

47. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

48. Plaintiffs and the Class conferred a benefit on Defendant by providing their SPI to Defendant, as well as making monetary payments, in exchange for convenience in the purchase of Defendant's products and services.

49. Defendant appreciated, accepted and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and the Class as described herein.

50. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful and inequitable proceeds received by it.

51. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiffs and the Class.

THIRD CLAIM FOR RELIEF
Violation of the Hawaii Data Breach Notification Act
Haw. Rev. Stat. § 487N-1, *et seq.*
(On behalf of Plaintiffs and the Class)

52. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

53. Defendant is a "business" within the meaning of Haw. Rev. Stat. § 487N-1.

54. Defendant stored the "personal information" of Plaintiffs and the Class within the meaning of Haw. Rev. Stat. § 487N-1.

55. Defendant suffered a "security breach" within the meaning of Haw. Rev. Stat. § 487N-1.

56. Under Haw. Rev. Stat. § 487N-2(b), Defendant was required to notify the owners of the personal information retained by Defendant "immediately following discovery of the breach." Defendant violated this statute by waiting forty-nine days following the discovery of the breach and twenty-three days following the results of its forensic audit to notify Plaintiffs and the Class of the breach.

57. As a result of Defendant's failure to immediately notify Plaintiffs and the Class of the breach, or even provide notification in a reasonably timely manner, Plaintiffs and the Class have been harmed by having their SPI exposed for weeks without their knowledge, and, in some cases, members of the Class have accrued fraudulent charges they believe are attributable to Defendant's failure.

58. As a result, Defendant is liable to Plaintiffs and the Class for actual damages as well as reasonable attorneys fees under Haw. Rev. Stat. § 487N-3.

FOURTH CLAIM FOR RELIEF
Violation of the Hawaii Unfair Competition Law
Haw. Rev. Stat. § 480-2, *et seq.*
(On behalf of Plaintiffs and the Class)

59. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

60. Plaintiffs are consumers within the meaning of HRS Section 480-1 in connection with their transactions with defendant described herein.

61. Defendant engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services in violation of Haw. Rev. Stat. § 480-2, *et seq.*, including but not limited to the following:

a. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the SPI of Plaintiffs and the Class;

b. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of the SPI of Plaintiffs and the Class in violation of duties imposed by and public

policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by state and federal laws, including section 5 of the Federal Trade Commission Act (15 U.S.C. § 45);

c. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to Plaintiffs and the Class in a timely and accurate manner, in violation of Haw. Rev. Stat. § 487N-2(b);

d. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect the SPI of Plaintiffs and the Class from further unauthorized disclosure, release, data breaches, and theft.

62. The above unlawful and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

63. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the SPI of Plaintiffs and the Class and that risk of a data breach or theft was highly likely. Defendant's actions

in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class.

64. As a direct and proximate result of Defendant's unlawful, unfair and deceptive practices, Plaintiffs and the Class suffered, and will continue to suffer, an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their SPI.

65. Plaintiffs and the Class seek relief under Haw. Rev. Stat. § 480-13, including, but not limited to, injunctive relief, actual damages, statutory treble damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, respectfully seek from the Court the following relief:

a. Certification of the Class as requested herein;

b. Appointment of Plaintiffs as Class representatives and their undersigned counsel as Class counsel;

c. Award Plaintiffs and the proposed Class all available damages, restitution and disgorgement, including treble damages;

d. Award Plaintiffs and the proposed Class equitable, injunctive and declaratory relief, including the enjoining of Defendant's insufficient data protection practices at issue herein and Defendant's continuation of its unlawful business practices as alleged herein;

e. An order declaring that Defendant's acts and practices with respect to the safekeeping of SPI are negligent;

f. Award Plaintiffs and the proposed Class pre-judgment and post-judgment interest as permitted by law;

g. Award Plaintiffs and the proposed Class reasonable attorneys' fees and costs of suit, including expert witness fees; and

h. Award Plaintiffs and the proposed Class any further relief the Court deems proper.

DATED: Honolulu, Hawaii, June 1, 2018.

/s/ *Bridget G. Morgan*
JAMES J. BICKERTON
BRIDGET G. MORGAN
GREGORY M. NESPOLE
MICHAEL LISKOW
CARL MALMSTROM
RACHEL R. RICKERT

Attorneys for Plaintiffs JOSHUA BOKELMAN and SUCHANDRA THAPA, individually and on behalf of all others similarly situated